Abstract

The present invention describes methods and systems to perform hash algorithms as logic gate functions. It processes an N-bit block of data into the M-bit hash or message digest of the block in one (1) process cycle instead of the multiple cycles generally required. The minimum process time is the total propagation delay of an input block through the core logic for an implementing technology. A message requiring Y blocks to process would require no more than Y process (clock) cycles to produce the final hash value. This creates very simple and fast implementations of hash algorithms which enable them to be simply and easily integrated into any system.